REMARKS

Claims 1-30 were pending in the Application. Claims 1-12 are herein canceled without prejudice or disclaimer to the subject matter recited therein. Claims 13-30 are now pending in the Application. Claims 13, 19, and 25 are the independent claims.

Claim Rejections - 35 USC §102

In the Office Action, the Examiner rejected claims 1-6 under 35 USC §102 as being anticipated by Gullman et al. USPN 5,280,527 ("Gullman").

The Applicants have canceled claims 1-6. Thus, this rejection is now moot.

Claim Rejections - 35 USC §103

In the Office Action, the Examiner rejected claims 7-30 as being unpatentable over Gullman in view of Gennaro et al USPN 6,317,834 ("Gennaro").

Claims 1-12 are herein canceled. Therefore, this rejection of claims 7-12 is now moot.

Claims 13, 19, and 25 (the remaining independent claims) have been amended so as to expressly recite respective acts of "combining" at least two different factor-based values to form a cryptographic key.

Amended claim 13 now recites the following act:

> "combining the first cryptographic key, the possession value, and the biometric value to form a second cryptographic key."

Amended claims 19 and 25 now recite the following act:

"combining the possession-based data instance and the biometric value to form a cryptographic key."

It is respectfully submitted that neither Gullman nor Gennaro (independently or in combination) teach or suggest, expressly or implicitly, an act of combining at least two different factor-based values to form a cryptographic key.

Gullman teaches that biometric information can be provided as input for a device, which then generates a **security token** based on the biometric information (2:21-23, Gullman) and either time-varying information or a user-input challenge code (2:40-44, Gullman). In particular, Gullman expressly teaches the definition of a security token, which is clearly not a cryptographic key:

"...A security token is a non-predictable code derived from a private key, e.g. a unique fixed value, and a public key, e.g. a time varying value. For example, a password (fixed key) is encoded based upon time-variant information. Such token then is forwarded to the host which decodes the token back to a password. The token thus provides security during transmission to prevent the unique fixed value from being identified. Even if a perpetrator intercepts a token during transmission, reapplication of the intercepted token will not enable access to the host system because the time-varying "public key" will have changed. Thus, a PIN provides user identification, while a token provides transmission security." (1:32-45, Gullman)

Thus, Gullman defines a security token as a non-predictable code derived from a private key. In his example, a password is encrypted (encoded) with time-variant information, and thereafter forwarded to a host, which then decrypts (decodes) the token back to the password. Indeed, Gullman stresses that the purpose of a security token is to provide security during transmission to prevent the unique fixed value from being identified.

In contrast, claims 13, 19, and 25 expressly recite the combining of different factor-based values to form a cryptographic key, which is not a security token as specifically and unequivocally defined by Gullman. Indeed, the security token of Gullman is not a cryptographic key.

On the other hand, Gennaro teaches that a cryptographic key can be generated from a password, or from a random combination of answers provided by a user during a challenge/response session (See 1:67-2:5 and 2:27-2:31, Gennaro). Clearly, generating a cryptographic key from a password, which is a single data element, does not qualify as generating a key from at least two different factor-based values. And further, generating a key from multiple answers to challenge questions does not qualify either. Indeed, the multiple answers of Gennaro are of the same type (i.e., knowledge-based values). They are all knowledge-based values, not **different** factor-based values.

Therefore, neither Gullman nor Gennaro teach or suggest, expressly or implicitly, combining at least two **different** factor-based values to form a **cryptographic key**.

Further, combining the teachings of Gullman and Gennaro would not produce an act of combining at least two different factor-based values to form a cryptographic key. As noted above, Gullman teaches generating a **security token** (an encrypted password) based on biometric information, and either time-varying information or a user-input challenge code; and Gennaro teaches a cryptographic key formed from either a single value, or multiple values of the same type.

Thus, if one were to combine the teachings of Gullman with those of Gennaro, the result would be as follows: a cryptographic key formed from a single value, or from multiple values of the same type, with the cryptographic key then being encrypted for

transit by either time-varying information or a user-input challenge code. Unequivocally, this result does not qualify as combining at least two **different** factor-based values to form a **cryptographic key**.

Therefore, it is respectfully submitted that claims 13, 19, and 25 are patentably distinguishable over the cited prior art, and are now in condition for allowance. Thus, it is requested that this rejection now be withdrawn, and these claims passed to issue.

Further, for at least the reasons set forth above, claims 14-18, which depend from claim 13; claims 20-24, which depend from claim 19; and claims 26-30, which depend from claim 25 are patentably distinguishable over the cited prior art, and are now in condition for allowance. Therefore, it is respectfully submitted that this rejection be withdrawn, and these claims passed to issue.

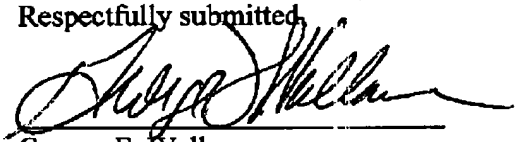
REQUESTED ACTION

The Applicants would like to thank the Examiner for his time and efforts during the September 25, 2003 interview, during which the undersigned and Examiner discussed distinctions between the claimed invention and the prior art.

The Applicant respectfully requests entry of the foregoing amendment, and withdrawal of the rejections for at least the foregoing reasons. Further, as the Applicants respectfully submit that claims 13-30 are patentably distinguishable over the prior art, and in condition for allowance, the Applicants respectfully request that claims 13-30 be passed to issue.

If the Examiner has any questions, or believes prosecution can be expedited, he is invited to telephone the undersigned counsel.

Respectfully submitted,



September 30, 2003
Date

George F. Wallace
Registration No. 45,286
IP STRATEGIES, P.C.
1730 North Lynn Street
Suite 500
Arlington , VA 22209
703.248.9220
703.248.9244 fax